

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
30 June 2005 (30.06.2005)

PCT

(10) International Publication Number
WO 2005/059725 A1

(51) International Patent Classification⁷: **G06F 1/00**, 12/14

(21) International Application Number:
PCT/GB2004/005327

(22) International Filing Date:
17 December 2004 (17.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03258079.7 19 December 2003 (19.12.2003) EP

(71) Applicant (for all designated States except US): **STMI-CROELECTRONICS LIMITED** [GB/GB]; 1000 Aztec West, Almondsbury, Bristol BS32 4SQ (GB).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **DELOW, Andrew**

[GB/GB]; 14 Tetbury Street, Minchinhampton, Gloucester GL6 9JG (GB). **GURNEY, Howard** [GB/GB]; C/o STMicroelectronics Limited, 1000 Aztec West, Almondsbury, Bristol BS32 4SQ (GB).

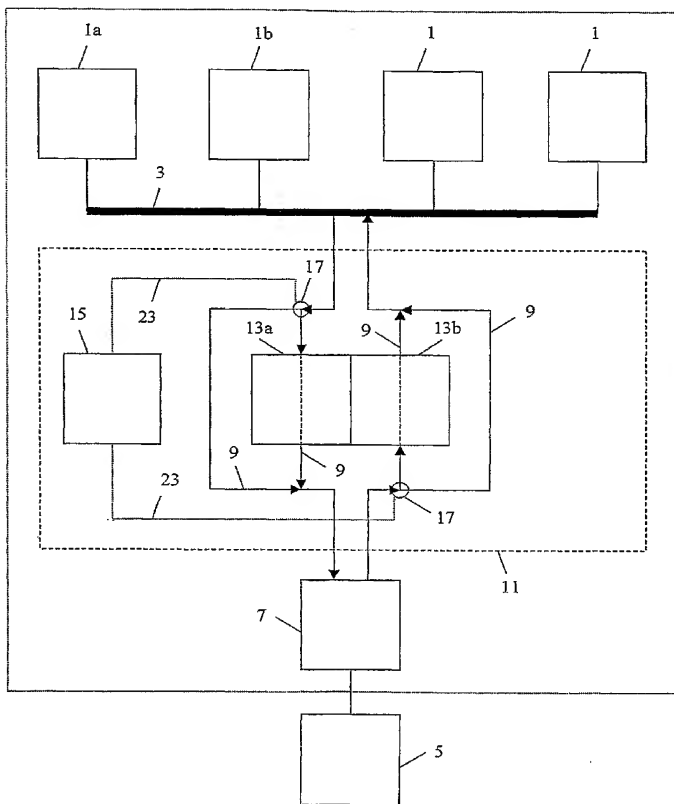
(74) Agent: **LOVELESS, Ian, Mark**; Reddie & Grose, 16 Theobalds Road, London WC1X 8PL (GB).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH,

[Continued on next page]

(54) Title: **MONOLITHIC SEMICONDUCTOR INTEGRATED CIRCUIT AND METHOD FOR SELECTIVE MEMORY ENCRYPTION AND DECRYPTION**



(57) Abstract: A monolithic semiconductor integrated circuit is provided for selectively encrypting or decrypting data transmitted between one of a plurality of devices on the circuit and an external memory. Two series of data pathways connect the devices and the external memory. The first series of data pathways passes through a cryptographic circuit causing data to be encrypted or decrypted, and the other series of data pathways provides an unhindered route. When a data access request is made by a device, the data is selectively routed along one of the two series of data pathways according to the identification of the device making the data access request. In one example, if data is transmitted from a device to the external memory, the data is selectively encrypted before being stored in the external memory if the device transmitting the data is identified as secure. Then, when that data is retrieved from the external memory by a second device, the data is selectively decrypted only if the second device is identified as secure.

WO 2005/059725 A1



GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.